AO 91 (Rev. 11/11) Criminal Complaint

SOUTHERN DISTRICT OF MISSISSIPPI
FILED
NOV 24 2015
ARTHUR JOHNSTON
BY DEPUTY

UNITED STATES DISTRICT COURT

for the

Southern District of Mississippi

United States of America
v.
Milad Kalantari

Defendant(s)

Case No. 1:15mj578-RHW

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 9/18/14 through 5/19/15 in the county of Harrison in the Southern District of Mississsippi, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §1349	Conspiracy to commit Bank Fraud.

This criminal complaint is based on these facts:

See affidavit attached hereto and incorporated herein by reference.

☑ Continued on the attached sheet.

[signature]
Complainant's signature

Brent Druery, Special Agent HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: Nov. 24, 2015

[signature]
Judge's signature

City and state: Gulfport, Mississippi

Robert H. Walker, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

After first being duly sworn, I, Brent Druery, do hereby state as follows:

1. I, Special Agent Brent Druery, am a duly sworn Special Agent (SA) with the Department of Homeland Security, Homeland Security Investigations, presently assigned to the Office of the Resident Agent in Charge, Gulfport, Mississippi (HSI Gulfport). I have been a Special Agent since November 2002.

2. Based upon my personal knowledge and information I have received from other law enforcement officials involved in the investigation, I am aware of the following facts:

3. HSI Gulfport is investigating Milad **KALANTARI**, an Iranian citizen residing in Iran, for numerous financial and identity theft crimes. This case was initiated following an investigation into the Yahoo Boys Criminal Organization, a West African transnational organized crime enterprise involved in numerous complex financial fraud schemes via the internet, including the use of stolen credit card information.

4. The investigation revealed that the Yahoo Boys were assisted in their schemes by Russian, Iranian, and Vietnamese cybercrime rings that are perpetuating the criminal underground economy, via the illegal sales of compromised or stolen credit card data and personal identifying information, via the internet. Investigation into the Yahoo Boys identified **KALANTARI**, utilizing the email accounts, miladrk@gmail.com and ccmilad@yahoo.com, as one of the suppliers of compromised credit card accounts and personal identifying information to the Yahoo Boys.

5. Through the course of the investigation, HSI Gulfport has executed numerous search warrants on the email accounts utilized by **KALANTARI**. Analysis of the email content revealed **KALANTARI** is the owner/operator of the websites miladccshop.biz and

miladccshop.ru. The aforementioned websites are dedicated to the sale of stolen credit card data. This includes stolen credit card data from citizens of the United States, United Kingdom, Canada, Australia, New Zealand, Italy, France, and other European countries. Analysis of the email content revealed the email accounts are being utilized to receive and distribute massive amounts of compromised credit card information and personal identifying information between **KALANTARI** and numerous co-conspirators. Analysis of the email content has also determined **KALANTARI** utilizes the email accounts to communicate with family members and conduct personnel business which has assisting in identifying **KALANTARI** as the user of the email accounts.

6. On February 8, 2013, **KALANTARI** received an online receipt from the purchase of a battery from batteryupgrade.de. The online receipt contained the following information regarding the purchase and shipping of the battery:

Name:	Milad Razaee KALANTARI
Address:	no 18, 3rd alley, andisheh st. Azadi blvd.
Zip Code:	4815774153
City:	Sari
Country:	Iran

7. Analysis of **KALANTARI's** email content also revealed his sister, Fatemeh Razaei Kalantari, is currently in the United States on a student visa. On April 6, 2014, **KALANTARI** received an email from his sister. Analysis of the email indicates Fatemeh applied to the University of Oklahoma State and needed a guarantee of financial resources in order to attend the university. On April 10, 2014, **KALANTARI** sent an email with attachment to Fatemeh. The attachment to the email contained a bank statement form **KALANTARI's** bank, Saman Bank. The bank statement contained the current balance as well as recent transactions. The attachment also contained a guarantor's certification in which **KALANTARI** identified himself as the brother of

Fatemeh and listed the following address:

No. 18, 3rd Alley, Andisheh St.
Azadi Blvd.
Sari, Mazandaran, Iran
Postal Code: 48157-74153

8. On May 7, 2015, during a Yahoo chat session with to one of his co-conspirators, r_arthur1985@yahoo.com, **KALANTARI** advised he won the United States Diversified State Lottery, allowing him to travel to the United States. In June 2015, SA Druery contacted the U.S. State Department, to verify **KALANTARI** had won the Lottery. The Department of State verified that **KALANTARI** had won the Diversified Lottery, allowing him to continue to pursue the visa and potentially travel to the United States as an immigrant. On November 20, 2015, the U.S. Embassy in Ankara, Turkey, verified that **KALANTARI** was scheduled for an interview on December 2, 2015, in regards to continue the visa application process.

9. On May 19, 2015, geochris_angel@yahoo.com sent an email to ccmilad@yahoo.com. The subject of the email was "16 fullz – 19 May." The email contained the name, full address, 16 digit credit card number, expiration date, and 3 digit card verification value (cvv) of 16 compromised bank cards. Included in this email was information pertaining to C.R., a resident of Gulfport, Mississippi. On October 8, 2015, SA Druery interviewed C.R. regarding fraudulent transactions associated with her card. SA Druery provided C.R. with the full 16 digit card number. C.R. identified the card as a Hancock Bank debit card previously assigned to C.R. C.R. advised the debit card was cancelled due to fraudulent activity. C.R. advised the fraudulent activity took place in approximately June 2015. C.R. could not recall the dollar amount of fraudulent activity on the card or where the fraudulent purchases occurred. C.R. advised she had not given anyone permission to utilize the card, withdraw funds, or make changes.

10. On March 14, 2015, ccmilad@yahoo.com sent an email to qhlove@gmail.com. The

subject of the email was "report shop 1." The email contained the last name, full address, 16 digit credit card number, expiration date, and 3 digit cvv of approximately 345 compromised bank cards. Included in the email was information pertaining to A.P., a resident of Gulfport, Mississippi. On September 16, 2015, SA Druery interviewed A.P. regarding fraudulent transactions associated with her card. SA Druery provided A.P. with the 16 digit card number. A.P. identified the card as a Keesler Federal Credit Union debit card previously assigned to her. A.P. advised the card was cancelled in March 2015 due to fraudulent activity. A.P. advised there were 4 unauthorized transactions on the card. A.P. advised each transaction was for $100 and occurred at Dunkin Donuts. A.P. advised she had not given anyone permission to utilize the card, withdraw funds, or make changes.

11. On October 18, 2014, boss_cvv_tk@yahoo.com sent an email to ccmilad@yahoo.com. The subject of the email was "651 us." The email contained the name, full address, email address, 16 digit credit card number, expiration date, and cvv of 651 compromised bank cards. Included in the email was information pertaining to Team One Communications, a business operating in Pascagoula, Mississippi. On September 16, 2015, SA Druery spoke with Christina Billings, manager for the Team One Communications bank card. SA Druery provided Billings with the 16 digit card number. Billings identified the card as a Coastal Bank and Trust card previously assigned to Team One Communications. Billings advised the card was cancelled by the bank after 3 attempted fraudulent transactions. Billings advised in October 2014, there were three attempted unauthorized transactions that were declined by the bank. Billings advised there were 2 attempted transactions for $20 and 1 attempted transaction for $100. Billings advised neither of the above attempted transactions were authorized by her or anyone else at Team One Communications.

12. Based on the experience of your affiant and the facts and circumstances described in this affidavit, it is believed by your affiant that Milad **KALANTARI**, has conspired with others known and unknown to the investigation to commit violations of: 18 U.S.C. 1349, Conspiracy to commit Bank Fraud.

Special Agent Brent Druery
Homeland Security Investigations

Sworn to and subscribed before me on the 24th day of November, 2015.

United States Magistrate Judge